



ANTI-EXECUTABLE

Umfassender Sicherheitsschutz,
dem Sie vertrauen können

Durch die Blockierung nicht autorisierter ausführbarer Dateien stoppen Sie Bedrohungen, bevor sie Ihnen gefährlich werden können

Die heutigen ausgereiften Bedrohungen wie Zero-Day-Angriffe, mutierende Malware und fortgeschrittene persistente Bedrohungen erfordern einen Ansatz, der über eine herkömmliche Antivirus-Lösung hinausgeht. Indem sichergestellt wird, dass nur zulässige Anwendungen auf einem Computer ausgeführt werden dürfen, geht die von Faronics Anti-Executable gebotene Sicherheit weit über das hinaus, was herkömmliche Antivirus-Lösungen bieten können: nicht autorisierte Programme – ganz gleich, ob sie schädlich, unlizenzziert oder einfach nur unerwünscht sind – werden an der Ausführung gehindert.

❑ SICHERHEIT AUF DEM ALLERNEUESTEN STAND DER TECHNIK

Schützt Benutzer vor unbekanntem Bedrohungen, beispielsweise vor Zero-Day-Angriffen, mutierender Malware, fortgeschrittenen persistenten Bedrohungen und raffinierten Angriffsformen.

❑ SCHUTZ VOR RANSOMWARE

Optimiert Systemeinstellungen, um Schwachstellen zu beseitigen und maximalen Schutz vor Ransomware-Angriffen zu bieten.

❑ GERINGERE BETRIEBSKOSTEN

Stellt sicher, dass Computer, Systeme und Bandbreite auch für den ihnen ursprünglich zugedachten Zweck verwendet werden.

❑ DETAILLIERTE KONTROLLE

Ermöglicht es Organisationen, sämtliche Vorteile einer Anwendungskontrolle wie z.B. herausgeberbasierte Genehmigungen, richtlinienbasierte Kontrollen oder Schutz auf lokaler Rechnerebene, auszuschöpfen.

❑ STEIGERUNG DER PRODUKTIVITÄT IHRER IT

Steigert die Produktivität der IT durch eine automatisierte Erstinstallation, eine standardisierte Konfiguration, eine zentrale Verwaltung und eine geringere Anzahl von IT-Support-Tickets.

❑ VERWALTUNG ÜBER EINE WEB-BASIERTE KONSOLE

Sowohl Verwaltung als auch Bereitstellung und Konfiguration erfolgen über eine einzige web-basierte Konsole oder eine Mobilfunk-App.

Wussten Sie schon?

Antivirus-Anbieter benötigen

11,6 Tage, um neue Malware zu erwischen.

- Cyveillance

Deep Freeze Cloud

bietet eine integrierte Konsole, über die Sie Ihre Computer absichern, aktualisieren und verwalten können.

Scannen Sie den QR-Code,

um sich direkt für Deep Freeze Cloud anzumelden



Hauptmerkmale



ANWENDUNGSKONTROLLE

Anwendungs-Positivlisten zur Verhinderung von Malware-, Ransomware- und Zero-Day-Angriffen. Autorisierung oder Verhinderung der Ausführung der Dateitypen .exe, .scr, .jar, .bat, .com, .vbs, .dll und .ps1 auf der Basis von Hash-Werten, digitalen Signaturen und Herausgebern.



WARNMELDUNGEN IN ECHTZEIT

Definition von Alarmschwellen, so dass Administratoren bei nicht autorisierten oder böswilligen Aktivitäten proaktiv benachrichtigt werden können. Erhalt von Benachrichtigungen über die Verwaltungskonsolle, per E-Mail oder über die mobile App.



UMFASSENDES BERICHTSWESEN

Erzeugung von Berichten über Verstöße, blockierte Programme und Aktivitäten, unter anderem auch darüber, welche Programme und welche Computer die höchste Anzahl an Verstößen aufweisen.



INTERAKTIVES DASHBOARD

Prüfung von Informationen zu Anwendungsverletzungen im Zusammenhang mit einzelnen Dateien oder Computern und Ergreifung sachkundiger Maßnahmen unter Verwendung dynamischer und filterbarer Widgets und Raster. Treffen fundierter Entscheidungen darüber, wann die Bereitstellungsphasen gewechselt werden sollen.



AUSFÜHRUNGSKONTROLLLISTE

Verwendung mehrerer Kontrollebenen zur Erstellung einer Liste zulässiger oder blockierter Anwendungen, entweder zentral über verschiedene Richtlinien oder lokal auf dem Computer.



VERTRAUENSWÜRDIGE BENUTZER & GRUPPEN

Gewährleistung, dass Windows-Powernutzer oder -Gruppen frei von Einschränkungen sind, während andere durch angewandte Richtlinien eingeschränkt werden.



AUDITMODUS

Protokollierung aller Anwendungsstarts und Softwareinstallationen ohne Aktivierung des Schutzes. Mit der abgestuften Implementierungsoption können Sie erst dann zum teilweisen oder vollständigen Schutz übergehen, wenn eine umfassende Kontrollliste erstellt wurde.



VERTRAUENSWÜRDIGE HERAUSGEBER

Automatisierte Genehmigung aller Updates eines bestimmten Herausgebers wie Microsoft oder Adobe.



DEEP-FREEZE- UND AV-INTEGRATION

Wechselt bei einem Deep Freeze-Wartungsereignis automatisch in den Wartungsmodus. Die Integration mit Faronics Antivirus stellt sicher, dass der Erstinstallationsscan frei von Malware ist.

Abgestufte Implementierung

Lernen Sie aus Benutzerinteraktionen, erstellen Sie eine umfassende Kontrollliste und wechseln Sie vom Audit-Modus in den Teil- oder Vollschutzmodus.

1 PRÜFEN

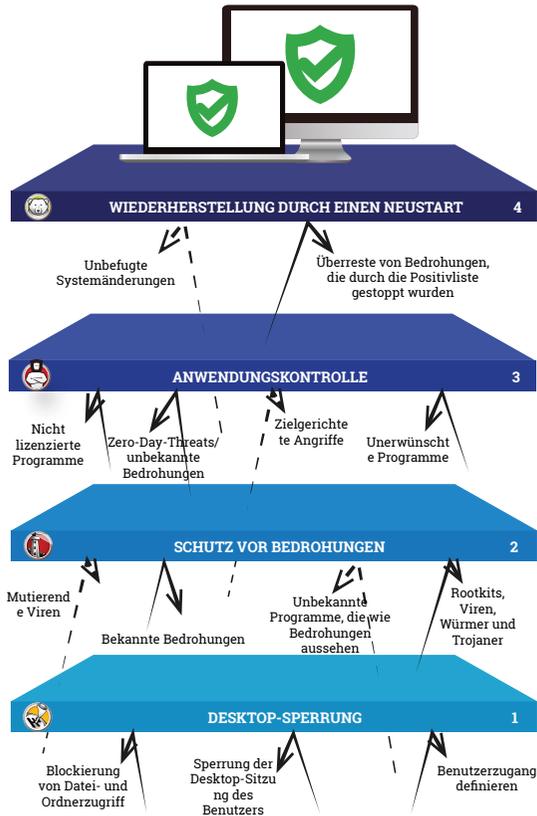
2 DURCHSETZEN

3 ÜBERWACHEN UND REAGIEREN

Faronics Anti-Executable trägt entscheidend zur Einsatzfähigkeit der wichtigsten Polizei-Computersysteme bei. Wir erreichen höchste Zuverlässigkeit und Sicherheit bei minimalen Ausfallzeiten. Der Einsatz von IT-Personal ist auf ein Minimum reduziert.

- Information and Communication Services Bureau des Los Angeles Police Departments

Die von Faronics Anti-Executable gebotene Sicherheit geht weit über das hinaus, was herkömmliche Antivirus-Lösungen bieten können: nicht autorisierte Programme – ganz gleich, ob sie schädlich, unlizenzziert oder einfach nur unerwünscht sind – werden an der Ausführung gehindert.



❑ FARONICS DEEP FREEZE

Patentierter Reboot-to-Restore-Technologie speichert den gewünschten Status Ihrer Endpunkte. Wiederherstellung nach unerwarteten Änderungen durch einen einfachen Neustart.

❑ FARONICS ANTI-EXECUTABLE

Schützt Benutzer vor unbekanntem Bedrohungen, beispielsweise vor Zero-Day-Exploits, mutierender Malware, fortgeschrittenen persistenten Bedrohungen und raffinierten Angriffsformen, indem nur zulässige Software erlaubt wird.

❑ FARONICS ANTI-VIRUS

Die leistungsfähige Anti-Malware-Engine überwacht aktive Anwendungen und ergreift ggf. sofort Gegenmaßnahmen. So bleibt keine Schadsoftware unerkannt, und das ohne Fehlalarme.

❑ FARONICS WINSELECT

Bieten Sie nur die beabsichtigte Windows-Funktionalität und kontrollieren Sie problemlos das Windows-Erlebnis Ihrer Endbenutzer, ohne sich mit GPOs auseinandersetzen zu müssen. Verhindert unzulässige Nutzung und schließt Sicherheitslücken.

SYSTEMANFORDERUNGEN

Windows 7 (32-Bit oder 64-Bit)

Windows 8.1 (32-Bit oder 64-Bit)

Windows 10 (32-Bit oder 64-Bit)



Damit wir Ihnen zeigen können, wie Ihre Rechnerumgebungen von den Lösungen von Faronics profitieren können, besuchen Sie uns unter www.faronics.com

USA

5506 Sunol Blvd, Suite 202
Pleasanton, CA, 94566 USA
Call Toll Free: 1-800-943-6422
Fax Toll Free: 1-800-943-6488
sales@faronics.com

CANADA

1400 - 609 Granville Street
PO Box 10362 Pacific Centre
Vancouver, BC, V7Y 1G5
Call Toll Free: 1-800-943-6422
Call Local: 1-604-637-3333
Fax Toll Free: 1-800-943-6488
sales@faronics.com

EUROPE

8 The Courtyard, Eastern Road,
Bracknell, Berkshire,
RG12 2XB, United Kingdom
Call Local: 44 (0) 1344 206 414
sales@faronics.eu

SINGAPORE

160 Robinson Road
#05-05 SBF Centre
Singapore, 068914
Call Local: +65 6509 4993
sales@faronics.com.sg